Recherche manuelle de générateurs de $\mathbb{F}_q^*$

Bruno Winckler

L'objectif de ce papier est de trouver un ou plusieurs générateurs des petits corps finis à la main. Pourquoi ? Pour l'amour du sport !

La stratégie générale s'appuie sur la formule

$$X^{p^n} - X = \prod_{d|n} \prod_{P \text{ irréductible sur } \mathbb{F}_p \text{ de degré } d} P,$$

que je ne démontrerai pas ici. Je ne considère que des polynômes irréductibles unitaires, évidemment. Je sais qu'un élément d'ordre q^n est racine de ce polynôme. Alors, en triant les racines des différents polynômes de la décomposition selon leurs ordres (par exemple, j'exclus les racines des $X^d - 1$ si ce polynôme apparaît dans la décomposition, pour $d < q^n - 1$, puisque ses racines sont d'ordre au plus d), j'espère trouver un générateur. Comme le pgcd de $X^n - 1$ et $X^m - 1$ est, en toute généralité, $X^{\mathrm{pgcd}(n,m)} - 1$, on est assuré qu'il apparaîtra dans ce produit. On pourrait chercher la factorisation de $X^{(p^n-1)/2} + 1$ directement (pour p impair), mais elle n'est pas connue *a priori*, donc plus compliquée.

Ceci ne marche pas pour les corps de la forme $\mathbb{F}_p$ où p est premier, puisque $X^p - X$ est, tout simplement, le produit de tous les éléments du corps, et ça revient à faire un test un par un. Pour ces corps, soit le générateur se trouve facilement, soit j'utilise la propriété suivante : si x et y sont d'ordres respectifs a et b, et que a et b sont premiers entre eux, alors xy sont d'ordre ab. Je note φ l'indicatrice d'Euler ; elle donne le nombre de générateurs d'un groupe cyclique.

Attention ! Pour les gros corps, je n'ai pas encore pris le temps de vérifier que les éléments que je trouve sont effectivement des générateurs avec toute la rigueur qui devrait être nécessaire.

Table des matières

1 Recherche des générateurs

1.1 Générateur de $\mathbb{F}_2^*$

L'élément 1 engendre trivialement $\mathbb{F}_2^*$.

1.2 Générateur de $\mathbb{F}_3^*$

L'élement -1 engendre trivialement $\mathbb{F}_3^*$.

1.3 Générateur de $\mathbb{F}_4^*$

Pour construire $\mathbb{F}_4$, j'ai besoin d'un polynôme de degré 2 irréductible sur $\mathbb{F}_2$. Je vérifie immédiatement que X^2+X+1 convient parce qu'il n'a pas de racine, donc $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1) = \{0, 1, j, 1+j\}$, où $j = \bar{X}$. Il n'y a que deux éléments à tester, à savoir j et $1+j$. Les deux conviennent : $j^3 - 1 = (j+1)(1+j+j^2) = 0$, donc $j^3 = 1$, et j est d'ordre 3 donc engendre $\mathbb{F}_4^*$. Comme $1+j = j^2$ est l'autre racine de X^2+X+1, on a le même résultat. En fait, sans même calculer, comme $\varphi(3) = 2$, il était garanti qu'ils engendrent le groupe multiplicatif.

1.4 Générateur de $\mathbb{F}_5^*$

En tâtonnant, on trouve que 2 engendre $\mathbb{F}_5^*$. En fait, -2 convient aussi. Comme $\varphi(4) = 2$, ce sont les seuls, comme on a vite fait de le remarquer.

1.5 Générateur de $\mathbb{F}_7^*$

Comme $\varphi(6) = 2$, on va peut-être tâtonner légèrement plus ; on peut essayer les éléments un par un. 2 est d'ordre 3, car $2^3 = 8 = 1$, et $2 \neq 1$. Comme -1 est d'ordre 2, et que 2 et 3 sont premiers entre eux, on en déduit que -2 est d'ordre 6, donc engendre $\mathbb{F}_7^*$.

1.6 Générateur de $\mathbb{F}_8^*$

Le groupe multiplicatif $\mathbb{F}_8^*$ est d'ordre premier, donc tout élément non trivial l'engendre. Indiquons tout de même que $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$.

1.7 Générateur de $\mathbb{F}_9^*$

Pour construire $\mathbb{F}_9$, j'ai besoin d'un polynôme de degré 2 irréductible sur $\mathbb{F}_3$. Je vérifie immédiatement que X^2+1 convient parce qu'il n'a pas de racine, donc $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$. Évidemment, $i = \bar{X}$ ne peut pas engendrer $\mathbb{F}_9^*$, parce qu'il est d'ordre 4. Pour trouver un générateur de son

groupe multiplicatif, encore une fois je passe par le polynôme $X^9 - X$: un générateur de $\mathbb{F}_9$ est une racine de ce polynôme, ou plus précisément de $X^8 - 1$. On a :

$$X^9 - X = X(X^4 - 1)(X^4 + 1) = X(X^4 - 1)(X^2 + X - 1)(X^2 - X - 1).$$

J'ai dû chercher les polynômes irréductibles de degré 2 pour trouver une factorisation de X^4+1 (les polynômes irréductibles apparaissant dans $X^4 + 1$ sont les seuls restants, puisque $X^2 + 1$ est facteur de $X^4 - 1$ et qu'il n'y en a que trois en tout), heureusement c'est facile. Un élément d'ordre 8 ne peut pas être racine de $X^4 - 1$, donc il est racine de $X^2 + X - 1$ ou $X^2 - X - 1$. Toutes les racines de ces polynômes conviennent, puisque $\varphi(8) = 4$, et qu'on tient là quatre racines. Il suffit donc de calculer une de leurs racines. Comme $X^2 + X - 1 = (X - 1)^2 + 1 = (X - 1)^2 - i^2$, ce polynôme admet pour racines dans $\mathbb{F}_9$ les éléments $1 + i$ et $1 - i$. L'autre polynôme admet comme racines $-1 + i$ et $1 + i$. On tient là tous les générateurs de $\mathbb{F}_9^*$.

1.8 Générateur de $\mathbb{F}_{11}^*$

En suivant la même stratégie que pour $\mathbb{F}_7^*$, si je trouve un élément d'ordre 5 (qui est premier à 2), c'est suffisant. Il y a quatre éléments d'ordre 5, et quatre éléments d'ordre 10, la recherche ne devrait donc pas être très longue : prenons 2, par exemple. On a $2^5 = 32 = -1$, donc $2^{10} = 1$, ouf !

1.9 Générateur de $\mathbb{F}_{13}^*$

Cette fois, il ne me suffit pas de trouver un élément d'ordre moitié, puisque 6 n'est pas premier à 2. L'élément 5 a un ordre facile à calculer : comme $5^2 = 25 = -1$, on a $5^4 = 1$, donc 5 est d'ordre 4. L'ordre de 3 est aussi facile à calculer, parce que $3^3 = 27 = 1$. Donc $15 = 2$ est d'ordre 12, et engendre $\mathbb{F}_{13}^*$. C'était plus rapide que de vérifier que $2^{12} = 1$.

1.10 Générateur de $\mathbb{F}_{16}^*$

Pour construire $\mathbb{F}_{16}$, j'ai besoin d'un polynôme de degré 4 irréductible sur $\mathbb{F}_2$. C'est assez simple : une condition nécessaire est qu'il n'ait pas de racine, et alors on doit juste éviter de prendre un polynôme de degré 4 qui s'écrit comme produit de deux irréductibles de degré 2. Or le seul irréductible de degré 2 sur $\mathbb{F}_2$ est $X^2 + X + 1$, le seul polynôme de degré 4 sans racine à éviter est donc $(X^2 + X + 1)^2 = X^4 + X^2 + 1$. Au choix, je peux prendre $X^4 + X^3 + 1$, $X^4 + X + 1$, ou encore $X^4 + X^3 + X^2 + X + 1$, qui est plus compliqué (mais pas nécessairement selon l'étude faite, puisque ses racines sont les éléments d'ordre 5 de $\mathbb{F}_{16}^*$) ; je vais donc l'éviter. Vous pouvez vérifier que ce sont les trois seuls, soit en montrant que les autres ont une racine, soit en calculant $I(4, 2)$, le nombre de polynômes irréductibles sur $\mathbb{F}_2$ de degré 4, à l'aide de la factorisation de $X^{q^n} - X$ donnée en introduction. On peut en effet trouver, si $I(n, q)$ est le nombre de polynômes irréductibles sur $\mathbb{F}_q$ de degré n :

$$I(n, q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},$$

où μ est la fonction de Möbius.

Soit donc $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)$. Pour trouver un générateur de son groupe multiplicatif, encore une fois je passe par le polynôme $X^{16} - X$: un générateur de $\mathbb{F}_{16}$ est une racine de ce polynôme, ou plus précisément de $X^{15} - 1$. On a :

$$X^{16} - X = X(X^5 - 1)(1 + X^5 + X^{10}).$$

Factoriser $1 + X^5 + X^{10}$ est un peu pénible. Heureusement, je sais déjà que tous les polynômes irréductibles de degré 4 doivent apparaître dans cette factorisation. Comme $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$, je sais d'ores et déjà que $1 + X^5 + X^{10}$ est produit des deux autres polynômes de degré 4, et d'un autre de degré 2 : c'est $X^2 + X + 1$.

Bref, $X^{16} - X = X(X^5 - 1)(X - 1)(X^4 + X^3 + 1)(X^4 + X + 1)(X^2 + X + 1)$; et je laisse volontairement $X^5 - 1$ sous cette forme, puisque je veux exclure les éléments d'ordre 5. Alors,

un élément d'ordre 15 de $\mathbb{F}_{16}$ est forcément une racine de $X^{10}+X^5+1$, donc de X^4+X^3+1, X^4+X+1 ou X^2+X+1. Mais ça ne peut pas être une racine de X^2+X+1, puisqu'une racine de X^2+X+1 est aussi une racine de $X^3-1=(X-1)(X^2+X+1)$, donc est d'ordre 3 (autre argument : les racines de X^2+X+1 engendrent $\mathbb{F}_4 \subseteq \mathbb{F}_{16}$, donc ne peuvent pas donner tout $\mathbb{F}_{16}$).

Donc $x=\bar{X}$, par exemple, engendre $\mathbb{F}_{16}$. Toutes les racines des deux polynômes de degré 4 ci-dessus engendrent $\mathbb{F}_{16}^*$: en effet, il y a $\varphi(15)=8$ générateurs, et on a exclu les racines des autres polynômes, il ne reste donc plus que ceux-là pour générer le groupe.

1.11 Générateur de $\mathbb{F}_{17}^*$

Heureusement, cet ensemble a « beaucoup » de générateurs : on a $\varphi(16)=8$. On a $2^4=16=-1$, donc 2 est d'ordre 8. Une racine carrée de 2 serait d'ordre 16... Et il en existe bien. En effet, soit ω une racine primitive huitième de l'unité dans une extension de $\mathbb{F}_{17}$, et posons $y=\omega+\omega^{-1}$. Cet élément vérifie $y^2=2$, donc est une racine carrée de y : en effet, comme $\omega^4=-1$, on a $\omega^2+\omega^{-2}=0$, d'où le résultat en développant $(\omega+\omega^{-1})^2$. De plus, le morphisme de Frobenius montre qu'on a $y^{17}=\omega^{17}+\omega^{-17}=\omega+\omega^{-1}=y$ car $\omega^8=1$, donc y appartient à l'ensemble des racines de $X^{17}-X$, qui est $\mathbb{F}_{17}$ (ce raisonnement est classique, il est inspiré par le fait que dans $\mathbb{C}$, l'élément $\zeta=\exp(2i\pi/8)$ vérifie $\zeta+\zeta^{-1}=\sqrt{2}$) ; ceux qui connaissent le symbole de Legendre auraient pu vérifier directement que $\left(\frac{2}{17}\right)=1$.

Mais ceci ne nous fournit pas notre racine carrée. On peut remarquer que $6^2=36=2$, et alors 6 est d'ordre 16, ouf.

Remarque. Voici un algorithme parmi d'autre pour trouver une racine carrée de 2, ou même de n'importe quel élément (en remplaçant si après 2 par un élément a qui est un carré) : je trouve un polynôme de la forme X^2-tX+2 qui est irréductible sur $\mathbb{F}_{17}$, en examinant son discriminant t^2-8. Par exemple, X^2-X+2 est irréductible (son discriminant est -7, or $\left(\frac{-7}{17}\right)=\left(\frac{17}{7}\right)=\left(\frac{3}{7}\right)=-1$), et soit x une racine de X^2-X+2 dans une extension de $\mathbb{F}_{17}$. Alors, x^{17} est aussi racine de ce polynôme (grâce à Frobenius !) en étant différent de x (car $x \notin \mathbb{F}_{17}$), donc $x^{18}=x\cdot x^{17}$ égale le coefficient constant du polynôme, à savoir 2. L'élément x^9 est une racine carrée de 2. Il ne reste plus qu'à calculer x^9, qui est bien un élément de $\mathbb{F}_{17}$, en faisant la division euclidienne de X^9 par X^2-X+2 : on obtient $X^9=(X^2-X+2)(X^7+X^6-X^5-3X^4-X^3+5X^2+7X-3)+6$, donc $x^9=6$.

1.12 Générateur de $\mathbb{F}_{19}^*$

Essayons avec 2. On a $2^5=32=13$, puis $2^6=26=7$, et $2^9=8\cdot 7=56=-1$, donc $2^{18}=1$. Ça marche !

1.13 Générateur de $\mathbb{F}_{23}^*$

2 est un carré dans $\mathbb{F}_{23}^*$ (par le même argument que dans $\mathbb{F}_{17}^*$; c'est en fait valable dès que le corps a un nombre d'éléments congru à $\pm 1 \mod 8$), donc d'ordre au plus 11, et en fait d'ordre exactement 11 car 2 n'est pas l'élément neutre. Alors, -2 est d'ordre 22, et engendre ce groupe.

1.14 Générateur de $\mathbb{F}_{25}^*$

On doit d'abord construire notre corps, en trouvant un polynôme irréductible de degré 2 sur $\mathbb{F}_5$; il suffit d'en trouver un qui n'a pas de racine. Le polynôme X^2+X+1 convient, encore une fois. Soit donc $\mathbb{F}_{25}=\mathbb{F}_5[X]/(X^2+X+1)$. On a :

$$X^{25}-X=X(X^3-1)(X^3+1)(X^6+1)(X^{12}+1)=X(X-1)(X^2+X+1)(X^3+1)(X^6+1)(X^{12}+1)$$

Comme $X^{25}-X$ s'écrit comme étant le produit de tous les polynômes irréductibles sur $\mathbb{F}_5$ de degré 1 et 2, $X^{12}+1$ s'écrit comme produit de six polynômes de degrés 2 (il est facile de se convaincre que $X^{12}+1$ n'a pas de racine sur $\mathbb{F}_5$, puisque tous les éléments de ce corps élevés à la puissance 4 donnent 1), et X^2+X+1 n'en fait pas partie. Il va donc falloir faire un peu de

recherche. Les polynômes irréductibles de degré 2 sont de la forme $X^2 \pm X \pm 1$, $X^2 \pm 2X \pm 1$, $X^2 \pm X \pm 2$, $X^2 \pm 2X \pm 2$, $X^2 \pm 2$ ou $X^2 \pm 1$, parce qu'ils ne sont pas divisibles par X, et seuls dix d'entre eux sont irréductibles. Il suffit de calculer leurs discriminants : si on tombe sur 0, 1 ou -1, les seuls carrés de $\mathbb{F}_5$, alors ils sont réductibles. En particulier si $X^2 + aX + b$ est irréductible, alors $X^2 - aX + b$ aussi. Voici la liste :

$$X^2 + X + 1, X^2 + 2X - 1, X^2 + X + 2, X^2 + 2X - 2, X^2 - 2,$$
$$X^2 - X + 1, X^2 - 2X - 1, X^2 - X + 2, X^2 - 2X - 2, X^2 + 2$$

Toujours grâce à la division euclidienne, on trouve que $X^{12} + 1$ est divisible par $X^2 - 2$. Plus précisément :

$$X^{12} + 1 = (X^2 - 2)(X^{10} + 2X^8 - X^6 - 2X^4 + X^2 + 2).$$

Un générateur du groupe s'obtiendra donc en résolvant l'équation $X^2 - 2 = 0$ dans $\mathbb{F}_{25}$ (on remarque que si on avait posé $\mathbb{F}_{25} = \mathbb{F}_5[X]/(X^2 - 2)$, ce serait plus facile...). Il ne nous reste plus qu'à déterminer $\sqrt{2}$. Cherchons-la sous la forme $ax + b \in \mathbb{F}_{25}$, avec $x = \bar{X}$. On a :

$$(ax + b)^2 - 2 = a^2x^2 + 2abx + b^2 - 2 = a^2(-x - 1) + 2abx + b^2 - 2 = (-a^2 + 2ab)x + (b^2 - a^2 - 2),$$

et ceci est nul pour $-a^2 + 2ab = 0$ et $b^2 - a^2 - 2 = 0$. La première égalité donne $-a + 2b = 0$, car $a \neq 0$ (sinon 2 serait un carré dans $\mathbb{F}_5$, mais ce n'est pas le cas), d'où $a = 2b$, puis $b^2 - a^2 - 2 = 0$ donne $-3b^2 - 2 = 0$, c'est-à-dire $2b^2 - 2 = 0$, puis $b = \pm 1$. La réciproque est immédiate. Donc $\pm(2x + 1)$ sont les racines de $X^2 - 2 = 0$, et engendrent $\mathbb{F}_{25}^*$.

Avec un peu d'intuition, on aurait pu trouver une racine de $X^2 - 2$ plus simplement, puisqu'il s'agit de trouver une racine de $2 = -3$. Comme $\mathbb{F}_{25} = \mathbb{F}_5[j]$, et que dans les nombres complexes on a $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, on en déduit $i\sqrt{3} = (2j + 1)$, puis $-3 = (2j + 1)^2$. On aurait alors trouvé heuristiquement $(2j + 1)$ comme racine de -3. C'est bien ce qu'on avait trouvé tout à l'heure.

Pour les curieux, voici la factorisation complète de $X^{12} + 1$:

$$X^{12} + 1 = (X^2 - 2)(X^2 + 2)(X^2 + 2X - 2)(X^2 - 2X - 2)(X^2 + X + 2)(X^2 - X + 2).$$

Remarque. J'ai, depuis, trouvé un moyen plus rapide de factoriser $X^{12} + 1$: en effet, on a

$$X^{12} + 1 = (X^2)^6 - 2^6 = (X^2 - 2)(X^{10} + 2X^8 + 2^2X^6 + 2^3X^4 + 2^4X^2 + 2^5),$$

ce qu'on avait effectivement trouvé précédemment.

1.15 Générateur de $\mathbb{F}_{27}^*$

Le polynôme $X^3 - X^2 + 1$ n'a pas de racine sur $\mathbb{F}_3$, donc est irréductible. Soit $\mathbb{F}_{27} = \mathbb{F}_3[X]/(X^3 - X^2 + 1)$. On a :

$$X^{27} - X = X(X^{26} - 1) = X(X^{13} - 1)(X^{13} + 1).$$

On sait également que ce polynôme est le produit de tous les irréductibles sur $\mathbb{F}_3$ de degré 1 ou 3. Il y a $I(3, 3) = \frac{27-3}{3} = 8$ polynômes irréductibles de degré 3. Si on en faisait la liste, et qu'on vérifiait lesquels divisent $X^{13} + 1$ (par division euclidienne par exemple), on pourrait alors poursuivre, en espérant trouver leurs racines, *etc.* Comme je suis paresseux, je vous laisse vous en occuper, et vais voir si $x = \bar{X}$ ne convient pas, tout simplement. Après tout, je ne cherche qu'un seul générateur ! En faisant la division euclidienne de $X^{13} + 1$ par $X^3 - X^2 + 1$ sur $\mathbb{F}_3$, j'obtiens un reste nul. Plus précisément :

$$X^{13} + 1 = (X^3 - X^2 + 1)(X^{10} + X^9 + X^8 - X^6 + X^5 + X^4 - X^3 + X^2 + 1).$$

L'algorithme d'Euclide étant très efficace, je vous invite à le vérifier. Donc $x^{13} = -1$ et $x^{26} = 1$: l'élément x engendre le groupe multiplicatif $\mathbb{F}_{27}^*$ (on devrait aussi vérifier $x^2 \neq 1$, mais c'est clair).

1.16 Générateur de $\mathbb{F}_{29}^*$

À tâtons, on trouve que 3 engendre le groupe : $3^3 = 27 = -2$, donc $3^{27} = ((3^3)^3)^3 = (-8)^3$. Or $(-8)^3 = -8^3 = -64 \cdot 8 = -6 \cdot 8 = -48 = 10$. Enfin, $3^{28} = 3 \cdot 10 = 30 = 1$. Il faut encore vérifier que 3 n'est pas d'ordre 2, 4, 7 ou 14, et ça se fait difficilement mais sûrement.

1.17 Générateur de $\mathbb{F}_{31}^*$

On a $2^5 = 1$, donc 2 est d'ordre 5 (comme $31 \equiv \pm 1 \mod 8$, on sait déjà que 2 est un carré grâce au symbole de Legendre, donc d'ordre au plus 15), et $4^3 = 64 = 2$, donc $8^{15} = 1$, et 8 est d'ordre 3, 5 ou 15. Comme $8^2 = 2$ et alors $8^3 = 16$, 8 n'est pas d'ordre 3. De plus, $8^5 = 2 \cdot 16 = 1$, donc 8 est d'ordre 5. Si je trouve un élément d'ordre 6 ou un élément d'ordre 3 (en se rappelant que -1 est d'ordre 2 premier à 3 et 5), j'ai gagné. Je calcule les puissances de 5 : on a $5^2 = 25 = -6$, donc $5^3 = -30 = 1$, donc 5 est d'ordre 3. Alors, $-1 \cdot 5 \cdot 8 = -9$ est d'ordre $2 \cdot 3 \cdot 5 = 30$, donc engendre le groupe.

1.18 Générateur de $\mathbb{F}_{32}^*$

L'ordre de $\mathbb{F}_{32}^*$ est premier, donc tout élément non trivial engendre le groupe. Construisons tout de même le corps. Pour construire $\mathbb{F}_{32}$, j'ai besoin d'un polynôme de degré 5 irréductible sur $\mathbb{F}_2$. Il ne doit pas avoir de racines, et doit être différent des polynômes $(X^2+X+1)(X^3+X+1) = X^5+X^4+1$, et $(X^2+X+1)(X^3+X^2+1) = X^5+X+1$ (j'ai fait le produit des seuls polynômes de degré 2 et 3 irréductibles sur $\mathbb{F}_2$). Par exemple, X^5+X^2+1 convient. Soit $\mathbb{F}_{32} = \mathbb{F}_5[X]/(X^5+X^2+1)$.

La liste complète des polynômes irréductibles de degré 5 (il y en a $\frac{32-2}{5} = 6$) est la suivante :

$$X^5+X^2+1, X^5+X^3+1, X^5+X^4+X^3+X^2+1, X^5+X^4+X^3+X+1, X^5+X^4+X^2+X+1, X^5+X^3+X^2+X+1.$$

En effet, demander à ne pas être divisible par X impose la présence du 1, et demander à ne pas être divisible par $X+1$ impose la présence d'un nombre pair de monômes X^k avec $k > 0$. Après, il suffit de s'assurer qu'on ne tombe pas sur X^5+X+1 et X^5+X^4+1. Le compte est bon.

1.19 Générateur de $\mathbb{F}_{37}^*$

Ça devient long, mais je les ferai tous jusqu'à 128, coûte que coûte ! Ici j'ai de la chance, car 2 convient, une fois de plus : on a $2^{12} = 4096 = 396 = 26 = -11$, puis $2^{18} = 64 \cdot (-11) = 110 = -1$, et enfin $2^{36} = 1$; l'élément 2 ne peut pas être d'ordre 2, 3, 6 ou 9, parce qu'en alors, en élevant à une certaine puissance paire, on obtiendrait $2^{18} = 1$, ce qui est absurde ; je ne ferai pas ce raisonnement à l'avenir, mais il reste souvent valide. Il est clair que 2 n'est pas d'ordre 4 non plus.

1.20 Générateur de $\mathbb{F}_{41}^*$

L'élément 2 n'est pas un générateur : on vérifie que c'est un carré, donc d'ordre au plus 20, et en fait d'ordre 20. Comme 2 n'est pas premier à 20, on ne peut pas en déduire que -2 est d'ordre 40. Intéressons-nous aux puissances de 3 : on a $3^4 = 81 = -1$, puis $(3^4)^2 = 3^8 = 1$, donc 3 est d'ordre 8. L'élément 5 ne peut pas être un générateur, car c'est un carré : la loi de réciprocité quadratique nous montre :

$$\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Je n'ai pas essayé l'élément 4 parce qu'il vaut 2^2, donc est d'ordre 10. Par contre, je ne peux pas procéder ainsi pour 2 et 3, et je vais donc tester 6 : on a $6^{20} = 3^{20} = 3^{8 \cdot 2} \cdot 3^4 = -1$, puis $6^{40} = 1$, et on vérifie sans peine que 6 est d'ordre exactement 40, donc 6 engendre $\mathbb{F}_{41}^*$.

Remarque. Comme dans le cas de $\mathbb{F}_{17}^*$, je peux chercher une racine carrée de 2 à l'aide d'une racine de $X^2 - tX + 2$ pour t approprié. Par exemple, $X^2 - X + 2$ convient, parce qu'il est de discriminant -7, et $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$, donc -7 n'est pas un carré. Alors, x^{21} modulo $x^2 - x + 2$ est une racine carrée de 2 dans $\mathbb{F}_{17}$. On trouve ainsi $x^{21} = 24$. C'est un générateur du groupe multiplicatif.

1.21 Générateur de $\mathbb{F}_{43}^*$

On a

$$2^{11} = 2048 = 2150 - 102 = -102 = 27,$$

et $2^{-1} = 22$, donc

$$2^{10} = 27 \cdot 22 = -27 \cdot 21 = -3^4 \cdot 7 = 5 \cdot 7 = -8.$$

Enfin, $2^{21} = 2^{11} \cdot 2^{10} = -27 \cdot 8 = -6^3 = -36 \cdot 6 = 7 \cdot 6 = -1$, et bien sûr $2^{42} = 1$; 2 est d'ordre exactement 42 (vérification aisée) et engendre $\mathbb{F}_{43}^*$.

1.22 Générateur de $\mathbb{F}_{47}^*$

Comme 2 est un carré modulo 47, il n'est pas un générateur, étant d'ordre au plus 23, donc d'ordre exactement 23. Alors, -2 est un générateur de $\mathbb{F}_{47}^*$.

1.23 Générateur de $\mathbb{F}_{49}^*$

Comme -1 n'est pas un carré modulo 7, on peut écrire $\mathbb{F}_{49} = \mathbb{F}_7[X]/(X^2+1)$. Je cherche des racines de $X^{24}+1$ dans $\mathbb{F}_{49}$. On a, par exemple :

$$X^{24} + 1 = (X^8)^3 - 3^3 = (X^8 - 3)(X^{16} + 3X^8 + 9).$$

Je pense que personne ne veut trouver à chaud une racine huitième de 3, ou factoriser un polynôme « bioctotique », je vais donc chercher un polynôme irréductible de degré 2 qui divise $X^8 - 3$ (comme $X^{24} + 1$ est un facteur de $X^{49} - X$ qui s'écrit comme produit de polynômes irréductibles de degré 1 ou 2, c'est aussi le cas de $X^8 - 3$, et il n'a pas de diviseur de degré 1 parce qu'il n'a pas de racine dans $\mathbb{F}_7$). Par exemple, le polynôme X^2+X+3 est de discriminant $-11 = 3$, qui n'est pas un carré modulo 7, donc est irréductible. On vérifie qu'il est un diviseur en effectuant la division euclidienne de $X^8 - 3$ par $X^2 + X + 3$; on trouve

$$X^8 - 3 = (X^2 + X + 3)(X^6 - X^5 - 2X^4 - 2X^3 + X^2 + 5X - 1).$$

Il faut donc trouver une racine de X^2+X+3 pour avoir un générateur de $\mathbb{F}_{49}^*$. Son discriminant est $3 = -4 = (2i)^2$ (où $i^2 = -1$), donc ses racines sont $\frac{-1 \pm 2i}{2} = -4 \pm i$. Ceci suffit, parce que cet élément ne peut pas être d'ordre 1, 2, 3, 4, 6, ou 12, parce qu'alors on aurait $x^{24} = 1$; on a $x^8 = 3 \neq 1$ et $x^{16} = 9 \neq 1$.

1.24 Générateur de $\mathbb{F}_{53}^*$

1.25 Générateur de $\mathbb{F}_{59}^*$

1.26 Générateur de $\mathbb{F}_{61}^*$

1.27 Générateur de $\mathbb{F}_{64}^*$

Pour construire $\mathbb{F}_{64}$, je cherche un polynôme irréductible de degré 6 sur $\mathbb{F}_2$. Un polynôme de degré 6 sans racine sur $\mathbb{F}_2$ est soit le produit de trois polynômes irréductibles de degré 2 (c'est alors $(X^2 + X + 1)^3 = X^6 + X^5 + X^3 + X + 1$), soit le produit de deux polynômes irréductibles de degré 3 (les deux polynômes irréductibles de degré 3 sur $\mathbb{F}_2$ sont $X^3 + X^2 + 1$ et $X^3 + X + 1$, ce qui exclut trois polynômes de degré 6, $X^6 + X^5 + X^3 + X^4 + X + X^2 + 1$, $X^6 + X^4 + 1$ et $X^6 + X^2 + 1$). Il nous suffit à présent de trouver un polynôme de degré 6 sans racine sur $\mathbb{F}_2$, et différent des polynômes ci-dessus ; il sera irréductible. Par exemple, $X^6 + X + 1$ convient. On peut donc poser $\mathbb{F}_{64} = \mathbb{F}_2[X]/(X^6 + X + 1)$.

Remarque. On a une autre méthode pour trouver un polynôme irréductible de degré 6, que j'aurais pu utiliser avant, mais des moyens plus directs étaient aussi efficaces : le polynôme cyclotomique $\Phi_9 = \Phi_3(X^2) = X^6+X^3+1$ est irréductible sur $\mathbb{Z}$ et $\mathbb{Q}$, et même sur $\mathbb{F}_2$: soit β une racine primitive neuvième de l'unité dans une extension de $\mathbb{F}_2$, on a alors $\Phi_9 = \prod_{i \in (\mathbb{Z}/9\mathbb{Z})^*}(X - \beta^i)$, et un facteur

irréductible Q de Φ_9 dans $\mathbb{F}_2$ s'écrit $Q = \prod_{i\in I}(X - \beta^i)$ (avec $I \subseteq (\mathbb{Z}/9\mathbb{Z})^*$ évidemment). Comme il est à coefficients dans $\mathbb{F}_2$, on a $Q(X^2) = Q(X)^2$ (c'est-à-dire que ses coefficients soient invariants sous l'action du morphisme de Frobenius), si et seulement si $\prod_{ß\in I}(X^2 - \beta^{2i}) = \prod_{i\in I}(X^2 - \beta^i)$, si et seulement I est stable par multiplication par 2. Mais les parties stables par la multiplication par 2 sont les orbites de $(\mathbb{Z}/9\mathbb{Z})^*$ sous l'action de $< 2 >= (\mathbb{Z}/9\mathbb{Z})^*$ par multiplication à gauche, lesquelles sont de la forme $\{2^k x; k \in \mathbb{Z}\}$ et donc toutes de cardinal $\mathrm{card}(< 2 >) = 6$. Bref, Q a six facteurs de degré 1, donc est de degré 6, et $Q = \Phi_9$.

Plus généralement, soit Φ_n un polynôme cyclotomique dont on veut étudier la factorisation sur $\mathbb{F}_q$. Si n n'est pas premier à q, de plus grand commun diviseur une puissance p^k (avec p premier), alors $\Phi_n = \Phi_{n/p^k}^{p^k - p^{k-1}}$. Si n est premier à q, alors $q \in (\mathbb{Z}/n\mathbb{Z})^*$, et si on note r l'ordre de q dans ce groupe, alors Φ_n s'écrit comme produit de $\varphi(n)/r$ polynômes irréductibles, tous de degré r. On démontre ce cas avec le même argument que ci-dessus dans le cas $n = 9$ et $p = 2$.

1.28 Générateur de $\mathbb{F}_{67}^*$

1.29 Générateur de $\mathbb{F}_{71}^*$

1.30 Générateur de $\mathbb{F}_{73}^*$

1.31 Générateur de $\mathbb{F}_{79}^*$

1.32 Générateur de $\mathbb{F}_{81}^*$

1.33 Générateur de $\mathbb{F}_{83}^*$

1.34 Générateur de $\mathbb{F}_{89}^*$

1.35 Générateur de $\mathbb{F}_{97}^*$

1.36 Générateur de $\mathbb{F}_{101}^*$

1.37 Générateur de $\mathbb{F}_{103}^*$

1.38 Générateur de $\mathbb{F}_{107}^*$

1.39 Générateur de $\mathbb{F}_{109}^*$

1.40 Générateur de $\mathbb{F}_{113}^*$

1.41 Générateur de $\mathbb{F}_{121}^*$

Pour construire le corps à 121 éléments, j'ai besoin d'un polynôme irréductible de degré 2 sur le corps $\mathbb{F}_{11}$. Comme -1 n'est pas un carré modulo 11, le polynôme $X^2 + 1$ est irréductible. On a alors $\mathbb{F}_{121} = \mathbb{F}_{11}[X]/(X^2 + 1)$.

On a

$$X^{60} + 1 = (X^4)^{15} - (-1)^{15} = (X^4 + 1)\sum_{k=0}^{14}(-1)^{14-k}X^{4k}.$$

Il suffit donc de trouver une racine quatrième de -1 dans $\mathbb{F}_{121}$. Soit i la classe de X. Alors $i^2 = -1$, et dans $\mathbb{F}_{121}$, le polynôme $X^4 + 1$ se factorise en $\big(X^2 - i\big)\big(X^2 + i\big)$, et on n'a plus qu'à trouver une racine carrée de i (ou $-i$). Cette racine carrée, que je note $ai + b$, doit vérifier $(ai + b)^2 = i$, c'est-à-dire :

$$2abi + (b^2 - a^2) = i,$$

donc $ab = -5$ et $b^2 - 3a^2 = 0$, ou encore $b = \pm a$ et $ab = -5$ (le cas $b = a$ est exclu car -5 n'est pas un carré modulo 11), qui fournissent $a = \pm 4$ et $b = \mp 4$. Ainsi, $\pm 4(i - 1)$ est un générateur de $\mathbb{F}_{121}^*$.

Remarque. Si on a l'œil, on peut remarquer que sur $\mathbb{F}_{11}$, on a $X^4+1 = (X^2+3X-1)(X^2-3X-1)$. Si on a l'habitude de multiplier des polynômes de degré 2 « conjugués », ça peut venir à l'esprit, en remarquant que $X^4+1 = (X^2-1)^2+2X = (X^2-1)^2-(3X)^2$. Alors, il suffit de trouver les racines dans $\mathbb{F}_{121}$ des deux polynômes qui apparaissent, et on trouve par exemple, pour $X^2 + 3X - 1$,

les racines $\frac{-3\pm\sqrt{2}}{2}$. Il n'est pas difficile de trouver, à partir de $i^2 = -1 = 2 \cdot (-2^{-1}) = 2 \cdot 5$, que $\sqrt{2} = \frac{i}{\sqrt{5}} = \frac{i}{\pm 4} = \pm 3i$.

Remarque. Dans $\mathbb{C}$, une racine carrée de i est $\frac{1}{\sqrt{2}}(1+i)$. Or, dans $\mathbb{F}_{121}$, on a

$$\frac{1}{\sqrt{2}}(1+i) = (\pm 3i)^{-1}(1+i) = \mp 4i(1+i) = \mp 4(i-1).$$

C'est précisément ce qu'on a trouvé précédemment. Comment expliquez-vous cette analogie entre la situation complexe et des corps finis, déjà constatée auparavant ?

1.42 Générateur de $\mathbb{F}_{125}^*$

1.43 Générateur de $\mathbb{F}_{127}^*$

On a $2^7 = 1$, donc 2 est d'ordre 7 et -2 est d'ordre 14. De plus, $5^3 = -2$, donc 5 est d'ordre 42, et je n'ai plus qu'à calculer une racine cubique de 5 non je rigole.

1.44 Générateur de $\mathbb{F}_{128}^*$

Le groupe $\mathbb{F}_{128}^*$ est d'ordre premier, donc tout élément non trivial l'engendre.

2 Tables de Pythagore

Merci de signaler d'éventuelles coquilles dans les tables. Pour en détecter, on peut inspecter les points suivants :

- chaque élément du groupe multiplicatif du corps doit se trouver dans chaque ligne et colonne, une et une seule fois (pourquoi ?) ;
- la table doit être symétrique par rapport à la diagonale (pourquoi ?) ;
- pour les corps de caractéristique 2, chaque élément apparaît une et une seule fois sur la diagonale, et pour les autres corps, la moitié des éléments apparaissent, et exactement deux fois chacun (pourquoi ?).

À chaque fois, dans le corps $\mathbb{F}_{p^n}$, l'élément x désigne la classe de X modulo le polynôme de $\mathbb{F}_p[X]$ par lequel je quotiente dans la section précédente pour construire $\mathbb{F}_{p^n}$.

2.1 Table de $\mathbb{F}_2^*$

$\times$	1
1	1

2.2 Table de $\mathbb{F}_3^*$

$\times$	-1	1
-1	1	-1
1	-1	1

2.3 Table de $\mathbb{F}_4^*$

$\times$	1	j	$1+j$
1	1	j	$1+j$
j	j	$1+j$	1
$1+j$	$1+j$	1	j

2.4 Table de $\mathbb{F}_5^*$

$\times$	-2	-1	1	2
-2	-1	2	-2	1
-1	2	1	-1	-2
1	-2	-1	1	2
2	1	-2	2	-1

2.5 Table de $\mathbb{F}_7^*$

$\times$	-3	-2	-1	1	2	3
-3	2	-1	3	-3	1	-2
-2	-1	-3	2	-2	3	1
-1	3	2	1	-1	-2	-3
1	-3	-2	-1	1	2	3
2	1	3	-2	2	-3	-1
3	-2	1	-3	3	-1	2

2.6 Table de $\mathbb{F}_8^*$

$\times$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

2.7 Table de $\mathbb{F}_9^*$

$\times$	-1	1	x	$x+1$	$x-1$	$-x$	$-x+1$	$-x-1$
-1	1	-1	$-x$	$-x-1$	$-x+1$	x	$x-1$	$x+1$
1	-1	1	x	$x+1$	$x-1$	$-x$	$-x+1$	$-x-1$
x	$-x$	x	-1	$x-1$	$-x-1$	1	$x+1$	$-x+1$
$x+1$	$-x-1$	$x+1$	$x-1$	$-x$	1	$-x+1$	-1	x
$x-1$	$-x+1$	$x-1$	$-x-1$	1	x	$x+1$	$-x$	-1
$-x$	x	$-x$	1	$-x+1$	$x+1$	-1	$-x-1$	$x-1$
$-x+1$	$x-1$	$-x+1$	$x+1$	-1	$-x$	$-x-1$	x	1
$-x-1$	$x+1$	$-x-1$	$-x+1$	x	-1	$x-1$	1	$-x$

2.8 Table de $\mathbb{F}_{11}^*$

$\times$	-5	-4	-3	-2	-1	1	2	3	4	5
-5	3	-2	4	-1	5	-5	1	-4	2	-3
-4	-2	5	1	-3	4	-4	3	-1	-5	2
-3	4	1	-2	-5	3	-3	5	2	-1	-4
-2	-1	-3	-5	4	2	-2	-4	5	3	1
-1	5	4	3	2	1	-1	-2	-3	-4	-5
1	-5	-4	-3	-2	-1	1	2	3	4	5
2	1	3	5	-4	-2	2	4	-5	-3	-1
3	-4	-1	2	5	-3	3	-5	-2	1	4
4	2	-5	-1	3	-4	4	-3	1	5	-2
5	-3	2	-4	1	-5	5	-1	4	-2	3

2.9 Table de $\mathbb{F}_{13}^*$

$\times$	-6	-5	-4	-3	-2	-1	1	2	3	4	5	6
-6	-3	4	-2	5	-1	6	-6	1	-5	2	-4	3
-5	4	-1	-6	2	-3	5	-5	3	-2	6	1	-4
-4	-2	-6	3	-1	-5	4	-4	5	1	-3	6	2
-3	5	2	-1	-4	6	3	-3	-6	4	1	-2	-5
-2	-1	-3	-5	6	4	2	-2	-4	-6	5	3	1
-1	6	5	4	3	2	1	-1	-2	-3	-4	-5	-6
1	-6	-5	-4	-3	-2	-1	1	2	3	4	5	6
2	1	3	5	-6	-4	-2	2	4	6	-5	-3	-1
3	-5	-2	1	4	-6	-3	3	6	-4	-1	2	5
4	2	6	-3	1	5	-4	4	-5	-1	3	-6	-2
5	-4	1	6	-2	3	-5	5	-3	2	-6	-1	4
6	3	-4	2	-5	1	-6	6	-1	5	-2	4	-3